CLAIMS

1. A programmable logic device (PLD) comprising:
configurable logic configured by a configuration memory;
structure for receiving a bitstream from a source external to the PLD, wherein the bitstream includes unencrypted configuration bits and encrypted configuration bits;
a key memory for storing a decryption key;
a decryptor having a decryption algorithm for decrypting the encrypted configuration bits in the bitstream using the key, and thereby forming configuration data; and
structure for loading the configuration data into the configuration memory.

2. The PLD of Claim 1 wherein the unencrypted configuration bits are control bits and the encrypted configuration bits are configuration data bits.

3. A programmable logic device (PLD) comprising:
configurable logic configured by a configuration memory;
structure for receiving a bitstream from a source external to the PLD;
a key memory for storing a decryption key;
a decryptor having a decryption algorithm for decrypting data in the bitstream using the key;
structure for loading the decrypted data into the configuration memory;
structure for reading header information from the bitstream indicating whether the bitstream includes encrypted data; and
structure for directing the bitstream to the decryptor if the header information indicates the bitstream includes encrypted data and bypassing the decryptor if the header information indicates the bitstream does not include encrypted data.

4. The PLD of Claim 3 further comprising:

structure for reading back configuration from the configuration memory; and

structure for disabling the structure for reading back configuration when the header information indicates the bitstream includes encrypted data.

5. The PLD of Claim 3 further comprising:

structure for reconfiguring the PLD after the PLD has been configured; and

structure for disabling the structure for reconfiguring the PLD when the header information indicates the bitstream includes encrypted data.

6. A programmable logic device (PLD) comprising:

configurable logic configured by a configuration memory;

structure for receiving a bitstream from a source external to the PLD;

a key memory for storing a plurality of decryption keys, wherein the key memory includes a plurality of registers for storing the plurality of decryption keys;

a decryptor having a decryption algorithm for decrypting data in the bitstream using at least one of the keys; and

structure for loading the decrypted data into the configuration memory.

7. The PLD of Claim 6 wherein the decryptor reads from one of the registers for storing a plurality of decryption keys a value indicating whether another key will also be used for decryption.

8. The PLD of Claim 6 wherein the decryptor includes a circuit for aborting decryption if an attempt is made to use the keys differently from the way specified by the keys.

9. The PLD of Claim 6 wherein a key specifies whether it is a first, middle, last, or only key of a key set.

10. The PLD of Claim 6 wherein a key specifies whether it is a last key or not a last key of a key set.

11. The PLD of Claim 6 wherein the PLD reads an address of a key from the bitstream.

12. The PLD of Claim 6 wherein a first group of words in the bitstream is encrypted with a first key known to a first designer and a second group of words in the bitstream is encrypted with a second key known to a second designer.

13. The PLD of Claim 1 further comprising structure for placing the key memory into a secure mode and a non-secure mode, and wherein keys are loaded while the key memory is in the non-secure mode.

14. The PLD of Claim 13 wherein the keys can be read while the key memory is in the non-secure mode.

15. The PLD of Claim 14 wherein moving the key memory from the secure mode to the non-secure mode causes all keys to be erased.

16. The PLD of Claim 15 wherein moving the key memory from the secure mode to the non-secure mode also causes the configuration data to be erased.

17. The PLD of Claim 1 wherein the bitstream comprises a plurality of words of data, and the decryption algorithm uses both the key and a previously decrypted

word of the configuration data for decrypting a current word of the encrypted configuration bits.

18. In a PLD having a decryptor for decrypting an encrypted bitstream and a plurality of keys for use by the decryptor, a method of using the plurality of keys comprising:

providing a first key to a first designer for encrypting a first part of a design; and

providing a second key to a second designer for encrypting a second part of the design.

19. In a PLD having a decryptor for decrypting an encrypted bitstream and a key for use by the decryptor, a method of using the PLD comprising:

placing the PLD into a non-secure mode; and

loading the key into the PLD.

20. The method of using the PLD of Claim 18 further comprising:

placing the PLD into a secure mode after the step of loading the key.

21. In a PLD having a decryptor for decrypting an encrypted bitstream and a key for use by the decryptor, a method of using the PLD comprising:

placing the PLD into a non-secure mode;

loading the key into the PLD; and

operating the PLD in a non-secure mode.

22. The method of using the PLD of Claim 21 comprising:

placing the PLD into a secure mode after the step of operating the PLD in a non-secure mode.

23. The method of using the PLD of Claim 21 comprising the further step of:
generating a CRC checksum using a bitstream being loaded into the PLD.

24. The method of using the PLD of Claim 21 comprising the further steps of:
loading a bitstream including encrypted data into the PLD;
decrypting the encrypted data to generate configuration data; and
calculating a CRC checksum on the configuration data.

25. The method of using the PLD of Claim 21 comprising the further steps of:
loading a bitstream including encrypted data into the PLD;
calculating a CRC checksum on the encrypted data; and
decrypting the encrypted data to generate configuration data.

26. A programmable logic device (PLD) comprising:
configurable logic configured by a configuration memory;
structure for receiving a bitstream from a source external to the PLD;
a key memory for storing a decryption key;
a decryptor having a decryption algorithm for decrypting encrypted configuration bits in the bitstream using the key, and thereby forming configuration data; and
structure for loading the configuration data into the configuration memory.

27. The PLD of claim 26 wherein the structure for loading the configuration data into the configuration memory includes a CRC checksum calculation circuit.